UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/681,158	10/09/2003	Lawrence Gerard Dobranski	38898-0039	1841

7590 09/21/2007

Fraser D. Rowand
RIDOUT & MAYBEE LLP
Suite 2400
One Queen Street East
Toronto, ON M5C 3B1
CANADA

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
09/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

4

Office Action Summary	**Application No.** 10/681,158	**Applicant(s)** DOBRANSKI ET AL.	
	Examiner Paula W. Klimach	**Art Unit** 2135	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 07/06/07. The amendment filed on 07/06/07 have been entered and made of record. Therefore, presently pending claims are 1-34.

Response to Arguments

Applicant's arguments filed 07/06/07 have been fully considered and have been found persuasive.

Applicant argued that the previous office action did not indicate clearly the element that corresponded to the synchronization vector. This is not found persuasive. The registered crypt string as indicated in the applicant's arguments corresponds to the synchronization vector. The missing element, "...the step of generating an encryption signal based upon a session key and encrypting such a bitstream with the encryption signal" is taught by the newly cited references, Robert.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7, 8-14, 15-21, 22-23, and 25-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hawthorne (5,798,381) in view of Roberts (6,931,128 B2).

In reference to claims 1, 8, and 15, Hawthorne discloses a system and method that enables encrypted communication between two station wherein the apparatus when acting as a sender creates a mutual primitive from stored items of data to generate a random session key and encrypt the random session key in accordance with the mutual primitive for transmission of the encrypted session key to the recipient station (abstract). The method comprises creating, at the transmitting set, a bitstream (registered crypt string together with the encrypted main message), said bitstream including a synchronization vector (registered crypt string) derived from a session key, Random Session Key, (column 5 lines 45-49), wherein the definition of synchronization vector is as discloses on the applicants specification (page 15 paragraph 0052); using said encryption signal to identify said synchronization vector (column 5 lines 55-67), and synchronizing the encryption signal to encrypted bitstream based on identification of said synchronization vector to permit recovery of the bitstream from said encrypted bitstream (column 5 lines 50-55).

Howthorne does not disclose generating, at the transmitting set, an encryption signal based upon said session key and encrypting said bitstream with said encryption signal; transmitting said encrypted bitstream from the transmitting set to the receiving set; and generating, at the receiving set, said encryption signal based upon said session key and decrypting said encrypted bitstream.

Roberts discloses generating, at the transmitting set, an encryption signal based upon said session key and encrypting said bitstream with said encryption signal (parts 403-408 Fig. 4); transmitting said encrypted bitstream from the transmitting set to the receiving set (part 409 Fig

4); and generating, at the receiving set, said encryption signal based upon said session key and decrypting said encrypted bitstream (part 601-605 Fig. 6).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the bitsteam of Howthorne using the system of Roberts. One of ordinary skill in the art would have been motivated to do this because the system of Roberts generates a security key such as an encryption key so as to make it more difficult for eavesdroppers to identify the key (Roberts column 2 lines 10-15).

In reference to claims 2, 9, and 16 Hawthorne teaches a system wherein said synchronization vector comprises said session key (column 6 lines 1-7).

In reference to claims 3, 10 and 17, Hawthorne teaches a system wherein said step of decrypting includes applying a feedback cipher to said encrypted bit stream to obtain a decrypted output, and comparing said decrypted output with said session key (column 5 lines 20-24 in combination with column 6 lines 50-55).

In reference to claims 4, 11, and 18, Hawthorne teaches a system wherein said bitstream includes random bits followed by said synchronization vector, followed by voice data (the random session key of Fig. 7 in combination with column 4 lines 55-67 in combination with lines 31-33).

In reference to claims 5, 12, and 19 Hawthorne teaches a system including a first step of calculating said session key from a common seed value (Fig. 7 part 73 and 75).

In reference to claims 6, 13, and 20, Hawthorne teaches a system wherein said step of calculating said session key includes applying a first function to said common seed value to generate said session key (part 71 and 74 Fig. 7).

In reference to claims 7, 14, and 21 Hawthorne teaches a system further including a step of applying a second function to said session key to produce a new seed value for use in subsequent communications (column 4 lines 31-33).

In reference to claims 22 and 28. Hawthorne discloses a system and method that enables encrypted communication between two station wherein the apparatus when acting as a sender creates a mutual primitive from stored items of data to generate a random session key and encrypt the random session key in accordance with the mutual primitive for transmission of the encrypted session key to the recipient station (abstract). The method includes the steps of providing the transmitting set and the receiving set with a seed value and a predetermined first function (part 71 and 74 Fig. 7); at each of the transmitting set and the receiving set, applying the predetermined first function to the seed value to produce a session key (part 71 and 74 Fig. 7).

Howthorne does not disclose generating, at the transmitting set, an encryption signal based upon said session key and encrypting said bitstream with said encryption signal; transmitting said encrypted bitstream from the transmitting set to the receiving set; and generating, at the receiving set, said encryption signal based upon said session key and decrypting said encrypted bitstream.

Roberts discloses generating, at the transmitting set, an encryption signal based upon said session key and encrypting said bitstream with said encryption signal (parts 403-408 Fig. 4); transmitting said encrypted bitstream from the transmitting set to the receiving set (part 409 Fig 4); and generating, at the receiving set, said encryption signal based upon said session key and decrypting said encrypted bitstream (part 601-605 Fig. 6).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the bitsteam of Howthorne using the system of Roberts. One of ordinary skill in the art would have been motivated to do this because the system of Roberts generates a security key such as an encryption key so as to make it more difficult for eavesdroppers to identify the key (Roberts column 2 lines 10-15).

In reference to claims 23 and 29 Hawthorne teaches a system wherein said step of providing includes distributing said seed value to the transmitting set and the receiving set by a call server via the network (column 4 lines 55-60).

In reference to claims 25 and 30 Hawthorne teaches a system further including a step of applying a second function to said session key to produce a new seed value (Fig 7).

In reference to claims 26 and 31 Hawthorne teaches a system wherein said step of encoding the voice data includes the steps of generating a bit stream, wherein said bit stream includes a synchronization vector and the voice data, said synchronization vector comprising said session key, and encrypting said bit stream with said encryption signal to produce an encrypted bit stream (column 5 lines 20-24 in combination with column 6 lines 50-55).

In reference to claims 27 and 32 Hawthorne teaches a system wherein said step of decoding said encrypted bit stream includes the steps of decrypting said encrypted bit stream to produce a decrypted bit stream and comparing said decrypted bit stream with said session key to identify said synchronization vector (Fig. 7 part 73 and 75).

Claims 24 and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hawthorne and further in view of Roberts as applied in claims 22 and 28 and further in view of the book by Menezes (Handbook of Applied Cryptography).

In reference to claim 24, Hawthorne may disclose a cipher however, Hawthorne does not teach including a step of receiving an index from a call server, and wherein said step of applying the predetermined first function includes repeating application based upon said index.

Menezes discloses including a step of receiving an index from a call server (trusted courirer), and wherein said step of applying the predetermined first function includes repeating application based upon said index (page 21).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the one time pad in the system of Menezes in the system of Hawthorne. One of ordinary skill in the art would have been motivated to do this because the one time pad is proven unbreakable.

In reference to claim 33, Hawthorne does not teach a system wherein the encrypter includes an XOR operator.

Menezes discloses a system wherein the encrypter includes an XOR operator (page 21).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the XOR operator as taught by Menezes in the cipher function of Hawthorne. One of ordinary skill in the art would have been motivated to do this because the XOR operator is a simple operation and therefore fast.

In reference to claim 34 Hawthorne does not each a system wherein the decrypter includes an SOR operator.

Menezes discloses a system wherein the decrypter includes an XOR operator (page 21).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the XOR operator as taught by Menezes in the cipher function of Hawthorne. One of ordinary skill in the art would have been motivated to do this because the XOR operator is a simple operation and therefore fast.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KIM VU
RY PATENT EXAMIN
LOGY CENTER 21